Information & Communications Technology Department

Student ICT Policy 2006-2007

To allow for the effective use of Information & Communications Technology(ICT) faclities and the creation of a pleasant and safe working environment, each student using ICT facilities at CSN must observe the following points:

Access to ICT facilities and the colloge network is a privilege extended to you as a student of this institution and is NOT an automatic right

It is mandatory for all students to have their CSN ID card displayed in a prominent position at the workstation when using any computer. Any student who cannot provide their ID card for inspection on request may be asked to leave the facility

All students must log on using their own student name and password! Any student who uses another person's account will have their access privileges withdrawn indefinitely

If a student forgets their password they must report this fact to their coordinator immediately. Access privileges will not be restored until they do so

All students are required to log off following each timetabled session

Computers in this college may only be used by students actively engaged in college approved or course related work

All internet access is moderated and filtered via proxy. Inappropriate browsing of Internet sites, downloading/installing of non-commissioned software, transmission of illegal /defamatory or obscene material is not acceptable

Using personal computers to play games is explicitly forbidden

Using chat room facilities that are not college approved is explicitly forbidden

No food or drink is allowed in any room that hosts computers

Use of mobile phones in any of the college's computer rooms is prohibited

All computer rooms are classrooms! Students are therefore required to work at all times and avoid unnecessary disruption to other users of the facility

While using any ICT facility, each student is responsible for his/her actions and is accontable to all staff members of this college. If a member of staff observes any student in breach of college IT regulations, the offending student will be asked to cease that activity immediately and may face sanctions or further punitive measures.

Sanctions

Physical abuse of ICT equipment, misuse of the Internet and/or other computer facilities will result in the immediate withdrawal of access privileges for an indefinite period of time. In the event of a serious breach of college regulations, access privileges will only be restored following a meeting between the student, the course coordinator and the IT system administrator. Further punitive measures may also be incurred, i.e., suspension or expulsion from a course of study. The college also reserves the right to report any illegal activities to the approprate authorities.

Internet Legislation

The college will provide, on request, information on the following legislation relating to the use of the Internet which students can familiarise themselves with

Data Protection Act - Amendment (2003)

Copyright and Related Rights Act (2000)

Child Trafficking and Pornography Act (1998)

Interception Act (1993)

Using IT facilities outside of timetabled computer classes

Students are expressly forbidden to use ICT facilities for any other purpose than course related, educational work. The main computer room located on the upper level is a classroom and casual, unstructured and non-productive usage of computers in this facility is prohibited.

Open access to the computer facilities is provded Monday to Thursday from 4.00pm onwards

Students are not allowed to use the college computer facilities without due supervision

Students must display their CSN ID card beside them at all times when using the IT facilities outside of timetabled classes

If students wish to avail of computer facilities (where appropriate) in a computer room during non-timetabled classes in *their* timetables, they MUST seek the permission of the teacher taking classes in the facility at that time. Any such permission must be sought prior to a timetabled class commencing. Please note that permission is granted at the discretion of the teacher in question and may NOT always be given

Students who are granted access to a computer facility during non-timetabled classes are NOT allowed to seek instruction from teachers operating in the computer facility at that time

Peer-to-Peer File-sharing (P2P)

P2P file-sharing is defined as software that allows a user to share files with other users on the Internet. In this case the user’s PC is open to receive files and to send files to other users at their request. P2P is used extensively for exchanging music, videos and software and includes packages such as KaZa, BitTorrent, etc. While P2P applications can provide a useful means for exchanging information, they can also expose the user and/or the college to significant risks such as the following:

Breach of Copyright: When you use P2P systems, your computer effectively becomes a server which can be accessed by others over the network. They can then copy from the computer, music or video files or other material which you may have downloaded. Users of such systems have a responsibility for ensuring that they are not violating copyright when downloading material (songs etc.) or through allowing others to download from their PC. Unless they have explicit permission from the copyright owners, they may be in breach of the Copyright and Related Rights Act (2000).

Network Performance: The majarity of P2P files tend to be audio or video files and are therefore very large. If there is a lot of P2P traffic, it can lead to congestion on the network and result in a serious deterioration of ICT services generally.

Security: By using P2P applications, you are opening up your computer for access by unknown users throughout the world. You are therefore increasing significantly the risk of infection from viruses etc. This could cause large numbers of computers both within and outside of CSN to be infected or otherwise compromised. In addition, it could facilitate the theft of personal or confidential information from computers on the CSN network.

CSN reserves the right to disable access to P2P applications if there is any evidence that their continued use is likely to cause a degradation of network performance or security or there is a risk that it will expose the college to legal action. It also reserves the right, through the ICT department, to disconnect any computer and/or user from the network where there is evidence that the computer is being used in a manner which breaches copyright or data protection legislation or which puts the services available to other users at risk.

It is recognised that P2P applications can be used in many cases for legitimate purposes and nothing will be done to interfere with such use where permission has been sought and approved and adequate precautions are taken to protect network performance and security.